This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A computer system for receiving encrypted compressed content and for producing decrypted decompressed content based on the received encrypted compressed content, the system comprising:

a decryption element for developing a content key and for decrypting the content based at least in part on the developed content key; and

a decompression element ~~included within the decryption element~~ for decompressing the content based at least in part on the content key, the decryption element supplying the content key to the ~~included~~ decompression element,

wherein the content key is employed to decrypt the content and also to decompress the content,

wherein the decompression element has a plurality of adjustable parameters and wherein the decompression element employs the content key as at least one of the adjustable parameters,

wherein the decompression element includes a quantizer for performing a lossy quantization step, and wherein the quantizer is de-dithered according to the content key, [[and]]

wherein the decompression element includes an internal representation that includes DCT coefficients of macroblocks, and wherein such coefficients are de-scrambled and de-noised according to the content key, and

wherein the decryption element and the decompression element are closely physically related to one another so as to protect the content key as supplied by the

decryption element to the decompression element, such close physical relationship comprising one of the decompression element residing in a process address space of the decryption element on the computer system and the decryption element residing in a process address space of the decompression element on the computer system.

2. (Original) The computer system of claim 1 comprising:

a decryption element having an input for receiving the encrypted compressed content, the decryption element for decrypting the encrypted compressed content based at least in part on a content key to result in decrypted compressed content, and having an output for producing the decrypted compressed content; and

a decompression element having an input for receiving the decrypted compressed content, the decompression element for decompressing the decrypted compressed content based at least in part on the content key to result in decrypted decompressed content, and having an output for producing the decrypted decompressed content,

wherein a content thief that obtains the decrypted compressed content from the output of the decryption element cannot decompress the obtained decrypted compressed content by way of another decompression element without the content key.

3-8 (Canceled)

9. (Currently Amended) A computer system for receiving content and for producing encrypted compressed content based on the received content, the system comprising:

an encryption element for developing a content key and for encrypting the content based at least in part on the developed content key; and

a compression element ~~included within the encryption element~~ for compressing the content based at least in part on the content key, the encryption element supplying the content key to the ~~included~~ compression element,

wherein the content key is employed to encrypt the content and also to compress the content,

wherein the compression element has a plurality of adjustable parameters and wherein the compression element employs the content key as at least one of the adjustable parameters,

wherein the compression element includes a quantizer for performing a lossy quantization step, and wherein the quantizer is dithered according to the content key, [[and]]

wherein the compression element includes an internal representation that includes DCT coefficients of macroblocks, and wherein such coefficients are scrambled and noised according to the content key, and

wherein the encryption element and the compression element are closely physically related to one another so as to protect the content key as supplied by the encryption element to the compression element, such close physical relationship comprising one of the compression element residing in a process address space of the encryption element on the computer system and the encryption element residing in a process address space of the compression element on the computer system.

10. (Previously Presented) The computer system of claim 9 comprising:

a compression element having an input for receiving the content, the compression element for compressing the content based at least in part on a content key to result in compressed content, and having an output for producing the compressed content; and

an encryption element having an input for receiving the compressed content, the encryption element for encrypting the compressed content based at least in part on the content key to result in encrypted compressed content, and having an output for producing the encrypted compressed content,

wherein the encrypted compressed content from the output of the encryption element cannot be decompressed without the content key.

11-13 (Canceled)

14. (Currently Amended) A method for receiving encrypted compressed content and for producing decrypted decompressed content based on the received encrypted compressed content, the method comprising:

developing a content key in a decryption element;

decrypting the content in the decryption element based at least in part on the content key; and

decompressing the content in a decompression element ~~included within the decryption element~~ based at least in part on the content key, the decryption element supplying the content key to the ~~included~~ decompression element,

wherein the content key is employed to decrypt the content and also to decompress the content,

wherein decompression is based on a plurality of adjustable parameters and wherein decompression comprises employing the content key as at least one of the adjustable parameters,

wherein decompression is based on a quantizer for performing a lossy quantization step, and wherein decompression comprises de-dithering the quantizer according to the content key, [[and]]

wherein decompression is also based on an internal representation that includes DCT coefficients of macroblocks, and wherein such decompression comprises de-scrambling and de-noising such coefficients according to the content key, and

wherein the decryption element and the decompression element are closely physically related to one another so as to protect the content key as supplied by the decryption element to the decompression element, such close physical relationship comprising one of the decompression element residing in a process address space of the decryption element on the computer system and the decryption element residing in a process address space of the decompression element on the computer system.

15. (Original) The method of claim 14 comprising:

decrypting the encrypted compressed content based at least in part on a content key to result in decrypted compressed content; and

decompressing the decrypted compressed content based at least in part on the content key to result in decrypted decompressed content,

wherein a content thief that obtains the decrypted compressed content cannot decompress the obtained decrypted compressed content without the content key.

16-18 (Canceled)

19. (Currently Amended) A method for receiving content and for producing encrypted compressed content based on the received content, the method comprising:

developing a content key in an encryption element;

encrypting the content in the encryption element based at least in part on the content key; and

compressing the content in a compression element ~~included within the encryption element~~ based at least in part on the content key, the encryption element supplying the content key to the ~~included~~ compression element,

wherein the content key is employed to encrypt the content and also to compress the content,

wherein compression is based on a plurality of adjustable parameters and wherein compression comprises employing the content key as at least one of the adjustable parameters,

wherein compression is based on a quantizer for performing a lossy quantization step, and wherein compression comprises dithering the quantizer according to the content key, [[and]]

wherein compression is also based on an internal representation that includes DCT coefficients of macroblocks, and wherein such compression comprises scrambling and -noising such coefficients according to the content key, and

wherein the encryption element and the compression element are closely physically related to one another so as to protect the content key as supplied by the encryption element to the compression element, such close physical relationship comprising one of the compression element residing in a process address space of the encryption element on the computer system and the encryption element residing in a process address space of the compression element on the computer system.

20. (Original) The method of claim 19 comprising:

compressing the content based at least in part on a content key to result in compressed content; and

encrypting the compressed content based at least in part on the content key to result in encrypted compressed content,

wherein the encrypted compressed content from the output of the encryption element cannot be decompress without the content key.

21-23 (Canceled)

24. (Currently Amended) A computer-readable medium having computer-executable instructions thereon for receiving encrypted compressed content and for producing decrypted decompressed content based on the received encrypted compressed content, the instructions being organized into modules including:

a first module for developing a content key and for decrypting the content based at least in part on the developed content key; and

a second module ~~included within the first module~~ for decompressing the content based at least in part on the content key, the first module supplying the content key to the ~~included~~ second module,

wherein the content key is employed to decrypt the content and also to decompress the content,

wherein the second module decompresses based on a plurality of adjustable parameters and wherein the second module employs the content key as at least one of the adjustable parameters,

wherein the second module decompresses based on a quantizer for performing a lossy quantization step, and wherein the second module de-dithers the quantizer according to the content key, [[and]]

wherein the second module decompresses based on an internal representation that includes DCT coefficients of macroblocks, and wherein such second module de-scrambles and de-noises such coefficients according to the content key, and

wherein the first module and the second module are closely physically related to one another so as to protect the content key as supplied by the first module to the second module, such close physical relationship comprising one of the second module as instantiated

on a computer system residing in a process address space of the first module as instantiated on the computer system and the first module as instantiated on the computer system residing in a process address space of the second module on the computer system.

25. (Original) The medium of claim 24 comprising:

a first module for decrypting the encrypted compressed content based at least in part on a content key to result in decrypted compressed content; and

a second module for decompressing the decrypted compressed content based at least in part on the content key to result in decrypted decompressed content,

wherein a content thief that obtains the decrypted compressed content cannot decompress the obtained decrypted compressed content without the content key.

26-28 (Canceled)

29. (Currently Amended) A computer-readable medium having computer-executable instructions thereon for receiving content and for producing encrypted compressed content based on the received content, the method comprising:

a first module for developing a content key and for encrypting the content based at least in part on the developed content key; and

a second module ~~included within the first module~~ for compressing the content based at least in part on the content key, the first module supplying the content key to the ~~included~~ second module,

wherein the content key is employed to encrypt the content and also to compress the content,

wherein the first module compresses based on a plurality of adjustable parameters and wherein the first module employs the content key as at least one of the adjustable parameters,

wherein the first module compresses based on a quantizer for performing a lossy quantization step, and wherein the first module dithers the quantizer according to the content key [[and]]

wherein the first module compresses based on an internal representation that includes DCT coefficients of macroblocks, and wherein such first module scrambles and noises such coefficients according to the content key, and

wherein the first module and the second module are closely physically related to one another so as to protect the content key as supplied by the first module to the second module, such close physical relationship comprising one of the second module as instantiated on a computer system residing in a process address space of the first module as instantiated on the computer system and the first module as instantiated on the computer system residing in a process address space of the second module on the computer system.

30. (Original) The medium of claim 29 comprising:

a first module for compressing the content based at least in part on a content key to result in compressed content; and

a second module for encrypting the compressed content based at least in part on the content key to result in encrypted compressed content,

wherein the encrypted compressed content from the output of the encryption element cannot be decompress without the content key.

31-33 (Canceled)